

Compte rendu TP thème 2 : chapitre 3 : td1

Sommaire

Introduction	1
Exercice 1	2
Exercice 2	3
Exercice 3	3
Exercice 4	4
Exercice 5	4
Conclusion	5

Introduction

Dans ce TP, j'ai appris à vérifier si une information est fiable et à utiliser différents outils pour surveiller la sécurité d'un site. Au fil des exercices, j'ai évalué des sources, analysé un site web et découvert comment mettre en place une veille simple en cybersécurité.

Exercice 1

Pour mener une veille efficace, il faut être capable d'évaluer plusieurs aspects des informations recueillies. Le tableau suivant présente les principaux critères, leur définition et un exemple d'application.

Tableau – Critères d'évaluation d'une source d'information

Critère	Description	Exemple
Crédibilité de l'auteur	Vérifier que l'auteur est reconnu et compétent	Organisation internationale
Fiabilité de la source	S'assurer que le site est officiel/fiable	ANSSI ou site technique spécialisé
Objectivité	Information neutre, non orientée	Article à but informatif
Exactitude	Données vérifiées, factuelles	Analyse technique validée
Actualité	Informations récentes et mises à jour	Alertes de vulnérabilités
Pertinence	Informations utiles pour la cybersécurité	Exemple : analyse d'un site bancaire

Exercice 2

Type d'outil	Nom	Points forts	Limites
Collecte d'infos	Google Alert	Automatisation, gain de temps	Alertes parfois non pertinentes
Traitement	Excel	Analyse et tri des données	Compétences techniques nécessaires
Curation	OneNote	Classement clair des ressources	Deviens vite chargé si mal organisé
Partage	Google Docs	Edition à plusieurs, accès facile	Risque d'erreurs/manipulations

Exercice 3

En plus des outils proposés (Google Safe Browsing, URLVoid), j'ai identifié :

1. Sucuri SiteCheck : Analyse complète (malwares, blacklist, injections).
2. Qualys SSL Labs : Vérification approfondie du protocole SSL/TLS.

Exercice 4

Test effectué pour le site : OWASP ZAP (<https://www.intruder.io>)

Critère	Google Safe Browsing	URLVoid
Malware	Aucun code malveillant signalé	Aucun malware détecté
Spam	Pas d'association au spam	Aucun signalement
Phishing	Aucun comportement frauduleux détecté	Base de données : aucun cas
Réputation	Réputation correcte	Confirmée par plusieurs sources
Listes noires	Non présent sur liste noire	Non répertorié

Exercice 5

Suite à la modification frauduleuse du site M@Banque, il est indispensable de rassurer les clients et de renforcer la surveillance du site.

Pour cela, plusieurs actions peuvent être mises en place :

Contrôles automatisés de l'intégrité du site, via :

- OWASP ZAP
- W3AF

Vérifications régulières de réputation et de sécurité :

- Google Safe Browsing

- URLVoid

Mise en place d'une veille technologique continue permettant de suivre les évolutions du site et d'identifier rapidement les anomalies.

Ces mesures contribueront à renforcer la confiance des clients tout en garantissant un niveau de sécurité optimal.

Conclusion

Grâce à ce TP, j'ai mieux compris comment repérer des informations fiables et comment vérifier la sécurité d'un site avec des outils adaptés. Les tests et les actions proposées m'ont permis de voir concrètement comment prévenir certains risques et rassurer les utilisateurs. J'ai ainsi découvert que la veille est un outil simple et utile pour rester protégé.